Security assessment on a VXLAN-based network

Guido Pineda Reyes

MSc. Systems and Networking Engineering
University of Amsterdam

February 5, 2014

Outline

Outline

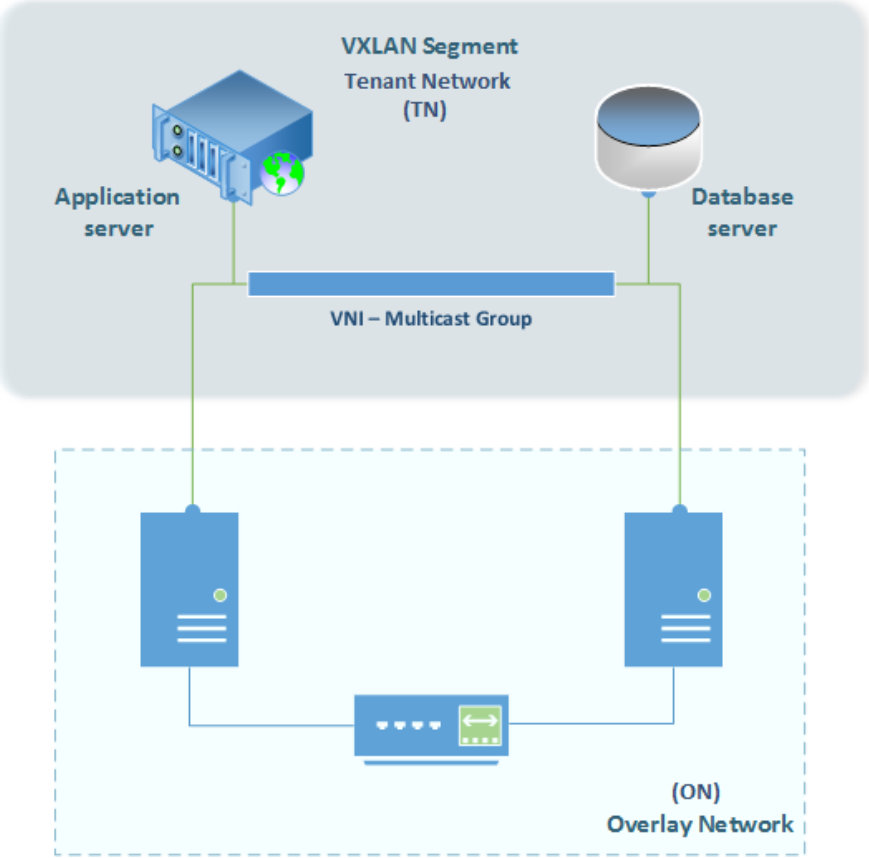
Virtual eXtensible LAN

Introduction

- Still an Internet Draft, current revision: 7th
- Allows to extend logical networks
- Encapsulates layer MAC-based Layer 2 frames within a UDP packet
- Up to 16 million logical networks
- Security measurements have not been performed yet

Virtual eXtensible LAN

Typical use case



Outline

Research questions

- Main question: How feasible are the known VLAN attacks in a VXLAN environment?
- Subquestions:
  - Which attacks were successful?
  - What is the difference between these attacks in a VLAN and a VXLAN environment?
  - Is there anyway to prevent them or mitigate them?

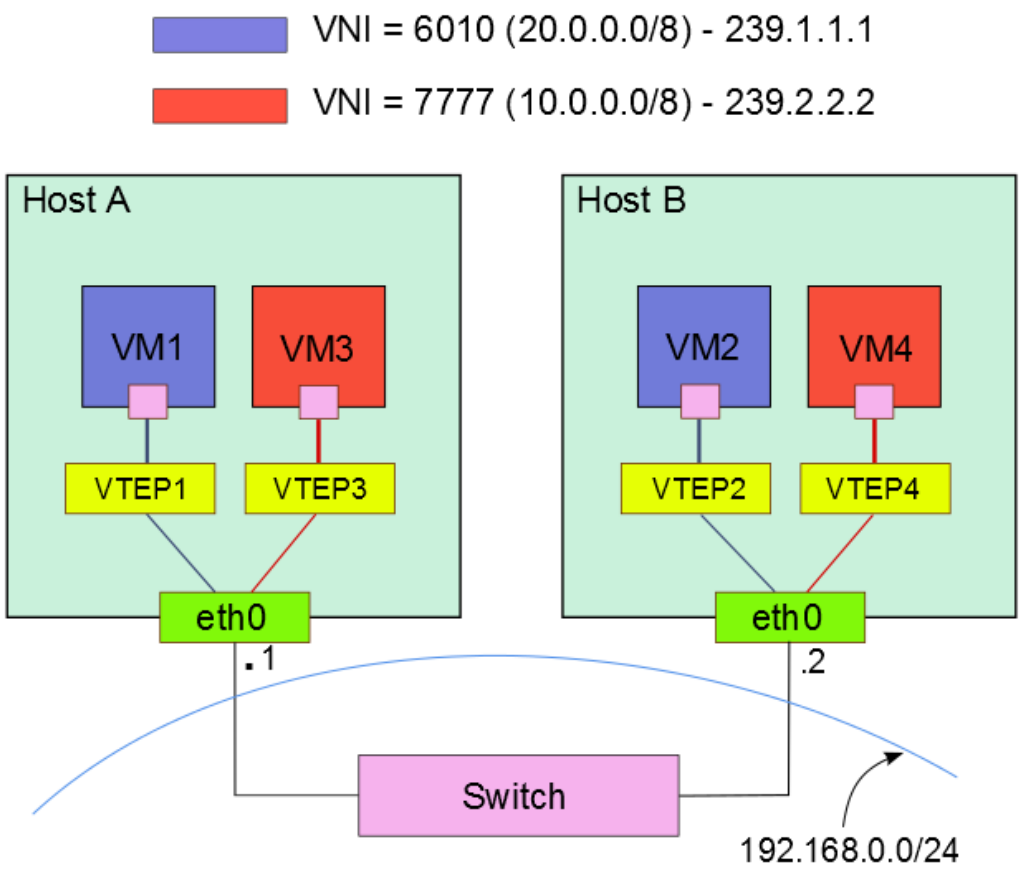
Outline

Approach

- Build the VXLAN prototype.
- Deploy the security assessment on the prototype.
- Focus on successful attacks.
- Understand how this attacks work to give a solution on how to mitigate or prevent them.

VXLAN prototype

Design



VXLAN prototype

Options

- VMware vSphere products
- VMware vSphere + Cisco Nexus 1000v
- VXLAN Linux implementation (needs kernel modification)

VXLAN prototype

Connectivity tests: UDP encapsulated traffic

247	55.149004000	192.168.0.1	192.168.0.2	UDP
248	55.149352000	192.168.0.2	192.168.0.1	UDP
249	55.149403000	192.168.0.2	192.168.0.1	UDP
250	55.149418000	192.168.0.2	192.168.0.1	UDP
251	55.149430000	192.168.0.2	192.168.0.1	UDP
252	55.149759000	192.168.0.1	192.168.0.2	UDP
253	55.149809000	192.168.0.1	192.168.0.2	UDP

VXLAN prototype

Connectivity tests: VXLAN encapsulation

```
⊞ Frame 436: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface 0
⊞ Ethernet II, Src: Parallel_b0:6e:42 (00:1c:42:b0:6e:42), Dst: Dell_8b:82:ab (b8:ac:6f:8b:82:ab)
⊞ Internet Protocol Version 4, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
⊞ User Datagram Protocol, Src Port: 56992 (56992), Dst Port: otv (8472)
⊟ Virtual eXtensible Local Area Network
  ⊞ Flags: 0x08
    Reserved: 0x000000
    VXLAN Network Identifier (VNI): 6010
    Reserved: 0
⊞ Ethernet II, Src: CadmusCo_19:49:23 (08:00:27:19:49:23), Dst: CadmusCo_82:35:ae (08:00:27:82:35:ae)
⊞ Internet Protocol Version 4, Src: 20.0.0.4 (20.0.0.4), Dst: 20.0.0.3 (20.0.0.3)
⊞ Internet Control Message Protocol
```

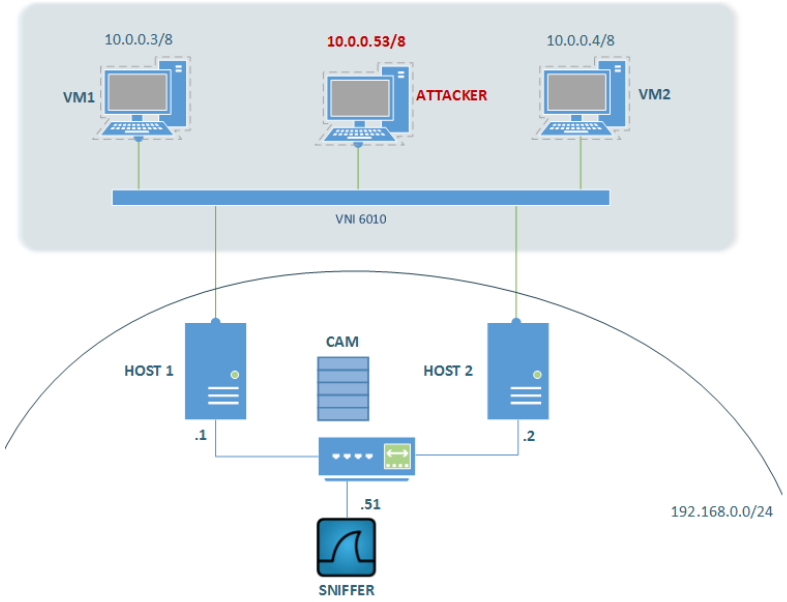
Security Assessment

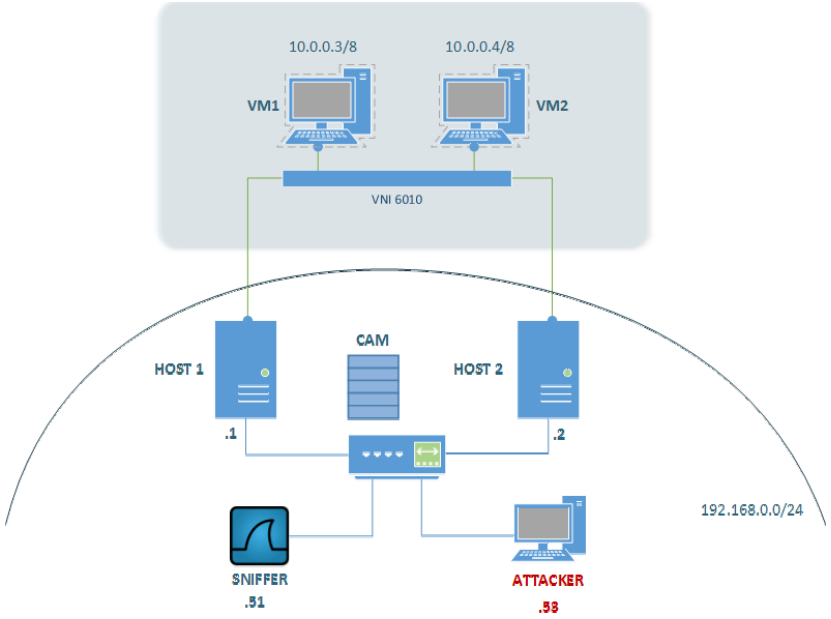
- MAC Flood Attack
- Double-Encapsulated 802.1Q/Nested VLAN Attack
- ARP Attack
- UDP Flood Attack
- Evaluation

Outline

MAC Flood Attack

Scenarios





MAC Flood Attack

- Tool: `macof`
- Results:
  - Attacker on physical net: Successful
  - Attacker on logical net: Failed
- Mitigation/Prevention:
  - Restrict the number of MAC addresses to one port
  - Specify static MAC address association
  - IDS

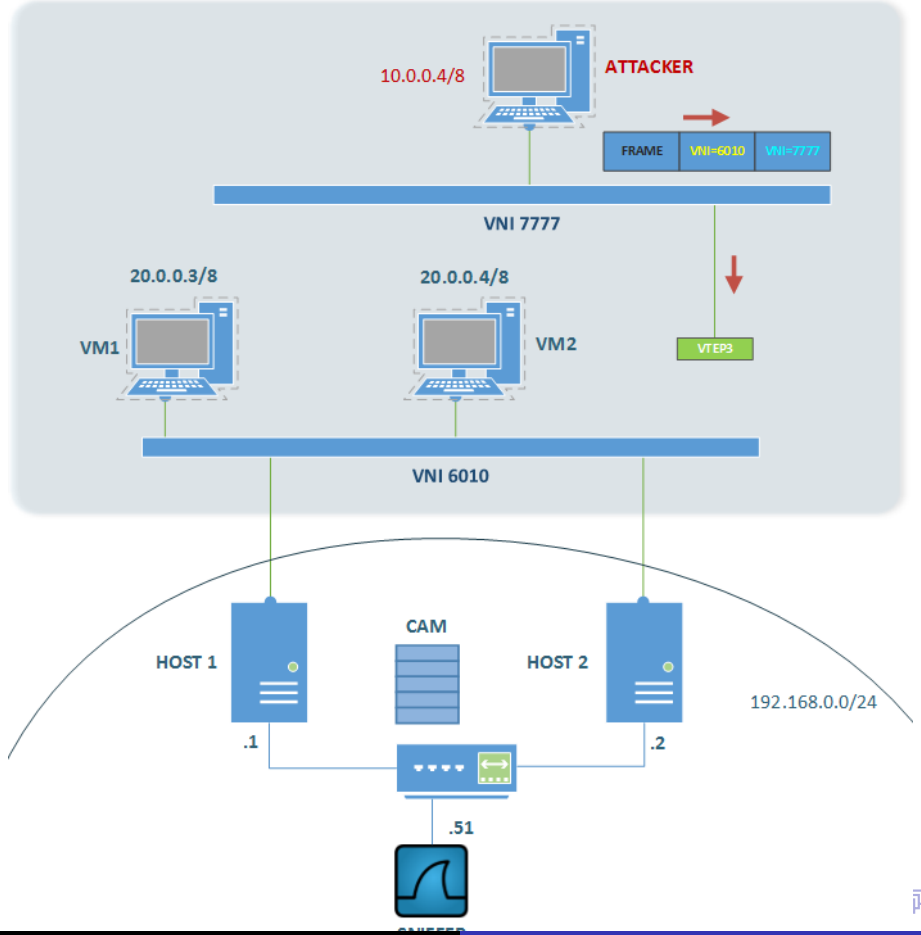
```
   1    f89f.094e.dbfe    DYNAMIC     Gi1/0/9
   1    f8e4.945f.e54e    DYNAMIC     Gi1/0/9
   1    fa92.480b.dc2f    DYNAMIC     Gi1/0/9
   1    fab1.d42b.8ed5    DYNAMIC     Gi1/0/9
Total Mac Addresses for this criterion: 6012
```

```
   1    001c.2381.aa2b    DYNAMIC     Gi1/0/11
   1    a820.6651.7a15    DYNAMIC     Gi1/0/9
   1    b8ac.6f8b.82ac    DYNAMIC     Gi1/0/1
Total Mac Addresses for this criterion: 24
```

Outline

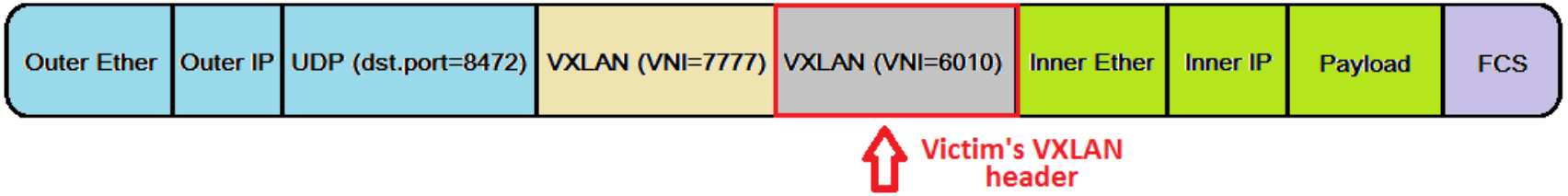
Double-Encapsulated 802.1Q/Nested VLAN Attack

Scenario



Double-Encapsulated 802.1Q/Nested VLAN Attack

Concept



Double-Encapsulated 802.1Q/Nested VLAN Attack

- Tool: `scapy`
- Results:
  - Attacker on logical net: Failed

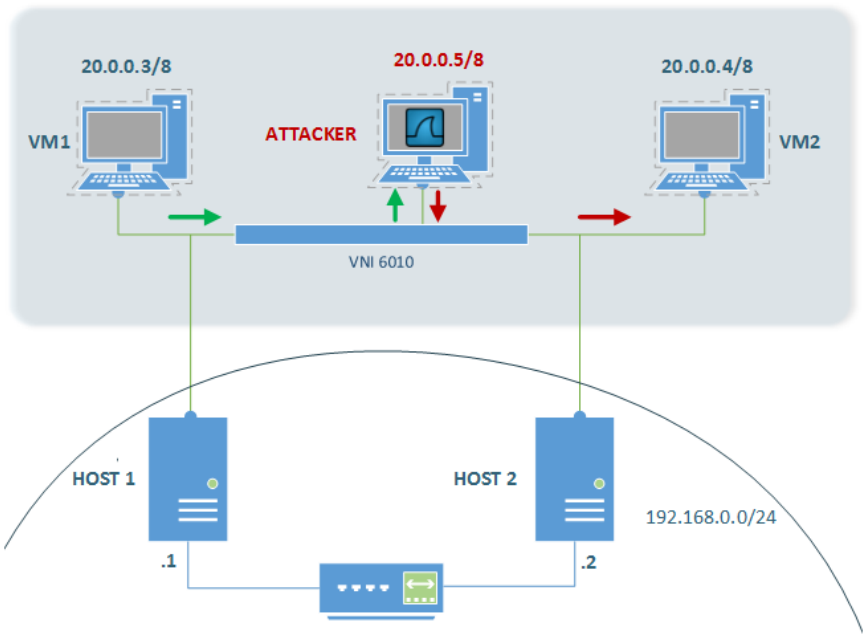
```
⊞ Frame 3: 92 bytes on wire (736 bits), 92
⊞ Ethernet II, Src: IntelCor_a8:25:8c (60:3
⊞ Internet Protocol Version 4, Src: 192.168
⊟ User Datagram Protocol, Src Port: menandm
    Source port: menandmice-dns (1337)
    Destination port: otv (8472)
    Length: 58
  ⊞ Checksum: 0x8734 [validation disabled]
⊟ Virtual eXtensible Local Area Network
  ⊞ Flags: 0x08
    Reserved: 0x000000
    VXLAN Network Identifier (VNI): 7777
    Reserved: 0
⊟ Ethernet II, Src: 7a:00:08:00:27:82 (7a:0
  ⊞ Destination: 08:00:00:00:00:17 (08:00:0
  ⊞ Source: 7a:00:08:00:27:82 (7a:00:08:00:
    Type: Unknown (0x35ac)
⊟ Data (28 bytes)
    Data: 08002719492308004500001400010000
    [Length: 28]
```

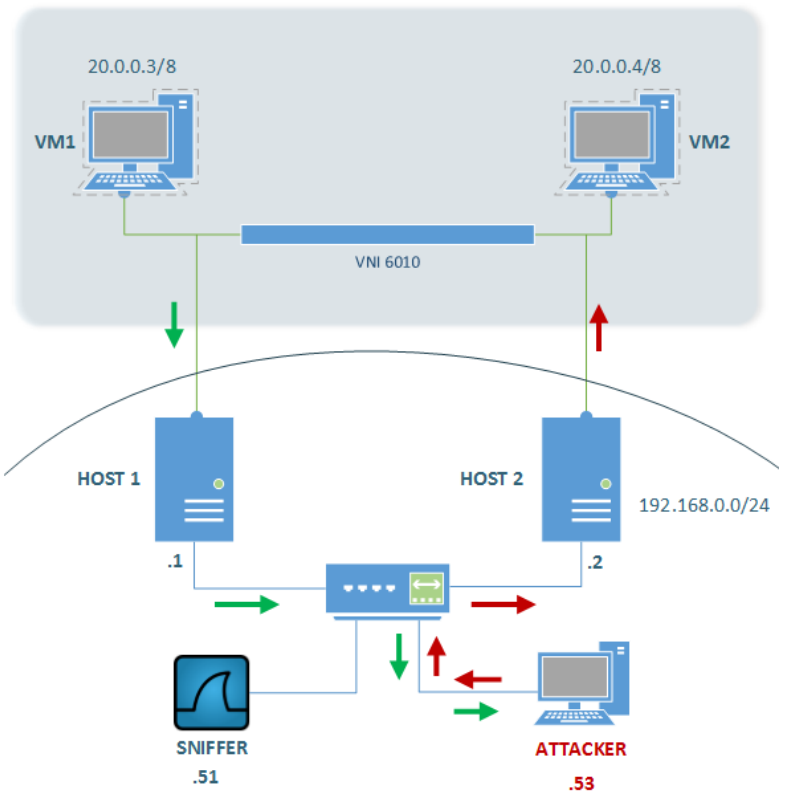
No double tagging

Outline

ARP Attack

Scenarios





ARP Attack

Summary

- Tool: `arpspoof`
- Results:
  - Attacker on physical net: Successful
  - Attacker on logical net: Successful
- Mitigation/Prevention:
  - Blocking direct communication between the attacker and the victim.
- Configuring private communication between the hosts at the service provider level.

```
vm2@VM2:~$ ping 20.0.0.3
PING 20.0.0.3 (20.0.0.3) 56(84) bytes of data.
64 bytes from 20.0.0.3: icmp_req=1 ttl=64 time=0.916 ms
64 bytes from 20.0.0.3: icmp_req=2 ttl=64 time=0.724 ms
From 20.0.0.5: icmp_seq=3 Redirect Host(New nexthop: 20.0.0.3)
From 20.0.0.5 icmp_seq=3 Redirect Host64 bytes from 20.0.0.3: ic
From 20.0.0.5: icmp_seq=4 Redirect Host(New nexthop: 20.0.0.3)
From 20.0.0.5 icmp_seq=4 Redirect Host64 bytes from 20.0.0.3: ic
From 20.0.0.5: icmp_seq=5 Redirect Host(New nexthop: 20.0.0.3)
```

Attacker IP Address

ARP Attack

Scenarios

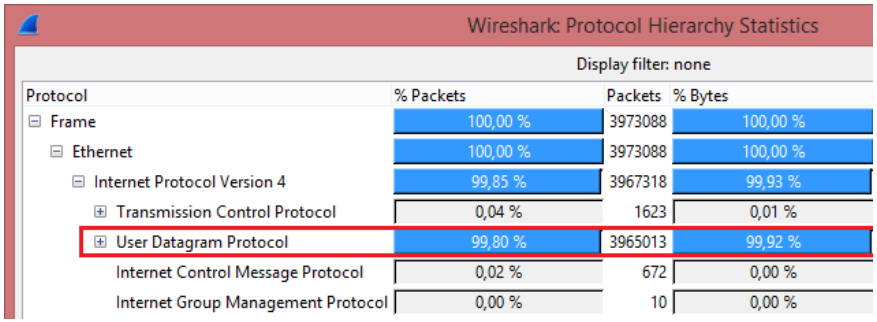
25	9.546994000	20.0.0.5	20.0.0.3	ICMP	126 Redirect
26	9.547013000	20.0.0.3	20.0.0.4	ICMP	98 Echo (ping) reply
27	10.001877000	CadmusCo_c1:09:db	CadmusCo_82:35:ae	ARP	42 20.0.0.4 is at 08:0
28	10.547709000	20.0.0.4	20.0.0.3	ICMP	98 Echo (ping) request
29	10.547745000	20.0.0.5	20.0.0.4	ICMP	126 Redirect

Outline

UDP Flood Attack

Summary

- Tool: `flood.pl`
- Results:
  - Attacker on physical net: Failed
- Mitigation/Prevention:
  - IDS to detect unusual UDP traffic


Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	% Bytes
Frame	100,00 %	3973088	100,00 %
Ethernet	100,00 %	3973088	100,00 %
Internet Protocol Version 4	99,85 %	3967318	99,93 %
Transmission Control Protocol	0,04 %	1623	0,01 %
User Datagram Protocol	99,80 %	3965013	99,92 %
Internet Control Message Protocol	0,02 %	672	0,00 %
Internet Group Management Protocol	0,00 %	10	0,00 %

Outline

Further research

Possible vulnerability

```
root@vtep1:~# bridge fdb show dev vxlan0
00:00:00:00:00:00 dst 239.1.1.1 via eth0 self permanent
ee:02:f4:3c:37:86 dst 192.168.0.2 self   ⇨ vxlan0 - Host 2
08:00:27:19:49:23 dst 192.168.0.2 self   ⇨ VM2 - Host2
root@vtep1:~# bridge fdb show dev vxlan1
00:00:00:00:00:00 dst 239.2.2.2 via eth0 self permanent
08:00:27:07:5b:82 dst 192.168.0.2 self   ⇨ VM6 - Host2
96:59:4e:9e:3c:02 dst 192.168.0.2 self   ⇨ vxlan1 - Host2
```

- Trying to modify the FDB and redirect all traffic to the attacker.

Outline

Conclusions

Most relevant points

Attack	Results: Scenario on		Tools
	Overlay Network	Tenant Network	
MAC Flooding Attack	Successful	Failed	macof
Double-Encapsulated/Nested VLAN Attack	N/A	Failed	scapy
ARP Attack	Successful	Successful	arpspoof
UDP Flood Attack	Failed	N/A	flood.pl

- Building the prototype is not trivial
- Some attacks are feasible
- Double-Encapsulation attack and MAC flooding attacks failures show that VXLAN segments are isolated from each other.
- ARP attacks show that Man in the Middle Attacks or DoS are possible from within any network (physical & logical).

Q&A

Questions?